PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/08 — A1

(11) Numéro de publication internationale: **WO 00/42731**

(43) Date de publication internationale: 20 juillet 2000 (20.07.00)

(21) Numéro de la demande internationale: PCT/FR00/00099

(22) Date de dépôt international: 18 janvier 2000 (18.01.00)

(30) Données relatives à la priorité:
99/00462 18 janvier 1999 (18.01.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F–92120 Montrouge (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: BUTNARU, Dan [FR/FR]; 61, rue des Longaines, F–91330 Yerres (FR). GELZE, Mathias [FR/FR]; 15, rue Poirier de Narçay, F–75014 Paris (FR). ROSSET, Raphaël [FR/FR]; 4, place du 11 Novembre, F–78220 Viroflay (FR).

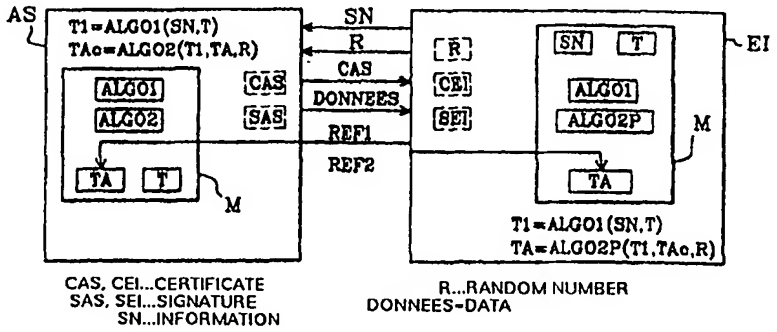
(74) Mandataire: UTZMANN–NORTH, Anne; Schlumberger Systèmes Test & Transactions, 50, avenue Jean Jaurès, Boîte postale 620–12, F–92542 Montrouge Cedex (FR).

(81) Etats désignés: CN, MX, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR SECURE DATA LOADING BETWEEN TWO SECURITY MODULES

(54) Titre: PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE



(57) Abstract

The invention concerns a method for customizing a security module comprising a secure loading of an application key from a first security module to a set of second security modules, said first and second security modules comprising each at least a storage unit. The invention is characterised in that said method comprises steps which consist, at each loading, in: calculating in the first and second modules an operating key from a transport key identical for each second module of said set; using the operating key for encrypting the application key in the first module; then sending the application key to the second module, decrypted and verified in said module. The operating key is not recorded in the storage unit of the security modules. The invention is particularly applicable in the field of banking.

(57) Abrégé

L'invention concerne un procédé de personnalisation de module de sécurité comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers un ensemble de plusieurs deuxièmes modules de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire. L'invention se caractérise en ce que ledit procédé comporte des étapes selon lesquelles, lors de chaque chargement, on calcule dans le premier et deuxièmes modules une clef d'exploitation à partir d'une clef de transport identique pour chaque deuxième module dudit ensemble. La clef d'exploitation est utilisée pour le chiffrement dans le premier module de la clef applicative. Cette dernière est par la suite envoyée au deuxième module, déchiffrée et vérifiée dans ledit module. La clef d'exploitation n'est pas enregistrée dans la mémoire des modules de sécurité. L'invention s'applique, en particulier au domaine bancaire.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

La présente invention concerne un procédé de personnalisation d'un ensemble de plusieurs deuxièmes modules de sécurité, comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers lesdits deuxièmes modules de sécurité dudit ensemble, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire.

L'invention trouve une application particulièrement avantageuse lors d'une phase de personnalisation de deuxièmes modules de sécurité dans les domaines tels que le domaine de la fidélité ou le domaine bancaire.

Un tel procédé de personnalisation est effectué avant une phase d'utilisation desdits deuxièmes modules. Par exemple, lors d'une phase d'utilisation dans le domaine de la fidélité, les deuxièmes modules se trouvent dans des terminaux de stations service et sont utilisés de manière à fournir des prestations de sécurisation de transactions de débit-crédit de points de fidélité entre un desdits terminaux et des cartes de crédit d'utilisateurs. Dans le domaine bancaire, les deuxièmes modules se trouvent dans des terminaux bancaires et fournissent des prestations de sécurisation de transactions d'argent dans des cartes de crédit d'utilisateurs.

Un état de la technique connu et divulgué dans le brevet américain publié sous le numéro US 5 517 567 au nom de DAQ Electronics enseigne qu'il existe un système de cryptage de clef dont le but est une sécurisation des communications pouvant s'établir entre un deuxième module de sécurité « master unit» et un troisième module utilisateur « remote unit » lorsque ce dernier est installé dans un site distant, par exemple dans un téléphone portable. Ladite sécurisation est basée sur l'utilisation d'une clef de communication temporaire.

Selon ce système, après que le module utilisateur est installé sur son site distant, on génère au moyen du deuxième module une clef de communication. Par suite, on envoie pour l'établissement de chaque communication, à partir du deuxième module au module utilisateur, la clef de communication chiffrée. La clef de communication permet un échange de messages sécurisés entre le deuxième module et le module utilisateur car elle n'est connue que de ces deux modules. En effet, ladite clef est basée sur une paire de deux nombres secrets unique à chaque module utilisateur et le deuxième module comporte toutes les paires correspondant à tous les modules utilisateurs. Le système est d'autant plus sécurisé qu'une paire de deux nombres secrets est inscrite dans la mémoire d'un module utilisateur, ladite mémoire étant volatile. Ainsi, lorsqu'une communication est terminée et lorsque le module utilisateur n'est plus alimenté, ladite paire est effacée et un fraudeur ne risque pas de découvrir les deux nombres secrets. Pour établir une autre communication, ledit système génère une autre clef de communication.

Le document cité ci-dessus décrit un système mis en oeuvre lors d'une phase d'utilisation d'un deuxième module et d'un module utilisateur, dont le but est d'établir une communication sécurisée entre les deux modules en utilisant une même clef de communication dédiée à une communication. Il ne décrit en aucune façon un système de personnalisation dont le but serait de sécuriser un chargement de clef dans un ensemble de plusieurs deuxièmes modules de sécurité.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de personnalisation d'un ensemble de plusieurs deuxièmes modules de sécurité comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers lesdits deuxièmes modules de sécurité dudit ensemble, lesdits premier et deuxièmes modules comprenant chacun au moins

une mémoire, qui permettrait, d'une part, d'éviter à un fraudeur de découvrir ladite clef applicative, et, d'autre part, de gagner du temps lors de la phase de personnalisation desdits deuxièmes modules de sécurité.

Une solution au problème technique posé se caractérise en ce que ledit procédé de personnalisation comporte les étapes selon lesquelles :

pour chaque deuxième module dudit ensemble,

- lors de chaque chargement, on calcule dans le premier module une clef d'exploitation à partir d'une information propre au deuxième module, d'une clef de transport et d'un algorithme de diversification, ladite clef de transport se trouvant dans la mémoire du premier module de sécurité, ladite mémoire étant non volatile,
- on chiffre dans le premier module la clef applicative, à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de cryptage, ladite clef applicative se trouvant dans ladite mémoire,
- on envoie au deuxième module des données comprenant la clef applicative chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module la clef d'exploitation à partir de l'information propre au deuxième module, de la clef de transport et de l'algorithme de diversification, ladite même clef de transport se trouvant dans la mémoire non volatile de chaque deuxième module de sécurité dudit ensemble, ladite clef d'exploitation n'étant pas enregistrée dans la mémoire dudit deuxième module,
- on déchiffre dans le deuxième module la clef applicative chiffrée, à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de décryptage inverse de l'algorithme de cryptage.

Ainsi, comme on le verra en détail plus loin, le procédé de chargement de l'invention permet, en calculant ladite clef d'exploitation et en ne la conservant que le temps du chiffrement ou du déchiffrement de la clef applicative, d'améliorer la sécurité du chargement d'une clef applicative. Par suite, un fraudeur ne pourra accéder à ladite clef d'exploitation ni par conséquent à la clef applicative. Les éventuelles fraudes sont par conséquent évitées et on n'effectue plus d'opérations qui sont coûteuses en temps pour la phase de personnalisation, le temps de calcul de la clef d'exploitation étant infime par rapport au temps d'accès nécessaire à l'enregistrement de ladite clef.

La description qui va suivre au regard des dessins annexés, donnée à titre d'exemple non limitatif, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant un premier module et plusieurs deuxièmes modules appartenant à un même ensemble.

La figure 2 est un schéma montrant le premier module et un deuxième module de la figure 1.

La figure 3 est un schéma montrant un échange de données entre le premier module et le deuxième module de la figure 2.

La figure 4 un schéma montrant un deuxième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 5 est un schéma montrant un troisième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 6 est un schéma montrant un quatrième échange de données entre le premier module et le deuxième module de la figure 2.

Sur la figure 1 est représenté un premier module AS de sécurité et plusieurs modules EI de sécurité d'un même ensemble S (non représenté), chacun des modules (AS,EI) comprenant au moins une mémoire M non volatile. Le premier module AS ainsi que les deuxièmes modules EI dudit ensemble S comportent une même clef T de transport

et un même algorithme ALGO1 appelé algorithme de diversification qui se trouvent dans la mémoire M. Sur la figure 2, sont représentés le module AS ainsi qu'un module EI dudit ensemble S. Chaque deuxième module EI de l'ensemble S comporte la même clef de transport T. Ainsi, on différencie un ensemble de deuxièmes modules EI d'un autre ensemble au moyen de ladite clef de transport T. Par exemple, deux ensembles de deuxièmes modules EI correspondent à deux fournisseurs de stations service différents.

En outre, le premier module AS comporte une clef applicative TA et un algorithme ALGO2 de cryptage. On notera que les deux algorithmes ALGO1 et ALGO2 peuvent utiliser un même algorithme de base. Chaque module EI dudit ensemble S comprend une information SN qui lui est propre et au moins une application utilisateur (non représenté), par exemple une application fournissant des prestations de sécurisations de transactions de débit-crédit de points de fidélité.

Afin d'utiliser les modules EI de sécurité dudit ensemble S, il faut pour chaque deuxième module EI dudit ensemble S, au préalable charger une clef applicative TA du premier module AS lors d'une phase dite de personnalisation comprenant les étapes décrites ci-après. Ladite clef est transférée par l'intermédiaire d'un réseau de communication standard. On empêche un fraudeur qui espionnerait ledit réseau ou lesdits modules d'accéder à des clefs des modules, comme décrit ci-après.

Dans une première étape, lors de chaque chargement, on calcule dans le premier module AS une clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite clef T de transport se trouvant dans la mémoire M du premier module AS de sécurité, ladite mémoire étant non volatile. Préférentiellement, ladite mémoire M est une mémoire réinscriptible. On notera que la clef de

transport T demeure valide même pendant les phases d'utilisation d'un deuxième module EI, tant qu'on ne la remplace pas.

L'information SN propre au deuxième module EI ne se trouve pas dans le premier module. Aussi, comme le montre la figure 3, on envoie au premier module AS l'information SN propre au deuxième module EI, préalablement au calcul dans le premier module AS de la clef T1 d'exploitation. Ledit premier module AS comporte préférentiellement plusieurs clefs applicatives TA. Ladite clef T1 va servir au chargement d'une des clefs applicatives TA contenues dans le premier module AS, ladite clef applicative choisie sera chiffrée et envoyée au module EI. Une clef applicative est associée à une application utilisateur. Suivant l'application se trouvant dans le deuxième module EI, on choisit la clef adéquate.

Comme le montre la figure 3, pour choisir une desdites clefs applicatives TA, dans une deuxième étape, on envoie au premier module AS une information REF1 relative à une clef applicative TA, préalablement au chiffrement dans ledit module AS de la clef applicative TA et on choisit la clef applicative TA à chiffrer à partir de ladite information REF1. On peut par exemple envoyer à partir du deuxième module EI une référence représentant un numéro de clef ayant une valeur de trois pour indiquer que l'on choisit la troisième clef correspondant à une application dudit module EI. C'est cette dernière qui sera chargée dans le deuxième module EI. S'il n'existe pas de clef applicative TA référencée par ledit nombre REF1, le premier module AS indique que ladite clef n'existe pas.

Dans une troisième étape, comme le montre la figure 3, on chiffre dans le premier module AS la clef applicative TA à partir d'informations comprenant ladite clef T1 d'exploitation et de l'algorithme ALGO2 de cryptage. Ladite clef d'exploitation se trouve temporairement dans une deuxième mémoire volatile (non représentée) du premier module AS.

Afin de protéger le premier module AS contre une éventuelle fraude, postérieurement au chiffrement de la clef applicative TA, on efface la clef T1 d'exploitation sauvegardée temporairement dans ladite deuxième mémoire volatile du premier module AS.

Après avoir chiffré ladite clef TA, on envoie au deuxième module EI des données DONNEES comprenant la clef applicative TA chiffrée.

Dans une quatrième étape, on déchiffre dans le deuxième module EI la clef applicative TA chiffrée, à partir d'informations comprenant ladite clef T1 d'exploitation et d'un algorithme ALGO2P de décryptage inverse de l'algorithme ALGO2 de cryptage. Dans cette étape, afin de retrouver la clef applicative TA choisie, il est nécessaire d'utiliser la même clef T1 d'exploitation qui a été utilisée pour le cryptage de ladite clef applicative TA dans le premier module AS de sécurité. A cette fin, préalablement au déchiffrement de la clef applicative TA chiffrée, lors de chaque chargement, on calcule dans le deuxième module EI la clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite même clef T de transport se trouvant dans la mémoire M non volatile de chaque deuxième module EI de sécurité dudit ensemble S, ladite clef T1 d'exploitation n'étant pas enregistrée dans la mémoire M d'un deuxième module EI. Préférentiellement la mémoire M du deuxième module est réinscriptible. Ladite clef T1 d'exploitation est sauvegardée temporairement dans une deuxième mémoire volatile (non représentée) du deuxième module EI.

On notera que ledit calcul peut se faire à tout moment avant le déchiffrement de la clef applicative TA. Les éléments nécessaires au calcul de la clef T1 d'exploitation dans le deuxième module EI de sécurité sont les mêmes que ceux utilisés pour le calcul de la clef T1 d'exploitation dans le premier module AS. Par conséquent, les deux clefs T1 sont identiques et on retrouve bien dans le deuxième module EI

la clef applicative TA choisie. Il n'a pas été nécessaire d'envoyer la clef T1 d'exploitation à travers le réseau de communication.

Dans une cinquième étape, postérieurement au déchiffrement de la clef applicative TA et préférentiellement juste après ledit déchiffrement, on efface la clef T1 d'exploitation sauvegardée temporairement dans ladite deuxième mémoire volatile du deuxième module EI.

Le fait, d'une part, de ne pas envoyer une clef d'exploitation T1 à travers le réseau de communication, d'autre part, de ne pas enregistrer une clef T1 d'exploitation dans une mémoire M non volatile d'un deuxième module EI, et enfin, le fait que ladite clef d'exploitation n'existe dans le deuxième module que le temps de déchiffrement de la clef applicative TA, rend une fraude plus difficile à effectuer dans la mesure où si un fraudeur veut trouver une clef applicative TA, il doit auparavant retrouver la clef T1 d'exploitation utilisée. Enfin, cela facilite la personnalisation et une mise sur le terrain d'un nième deuxième module EI dans la mesure où pour personnaliser les deuxièmes modules il n'est plus nécessaire d'effectuer deux chargements, un premier d'une clef T1 d'exploitation et un deuxième d'une clef applicative TA, mais simplement un chargement d'une clef applicative TA. On se libère ainsi de du premier chargement qui est habituellement effectué par une entité différente du premier module AS, ce qui complique généralement d'autant plus les choses.

A l'instar du premier module AS, un module EI comprend préférentiellement plusieurs clefs applicatives TA. Ainsi, au moyen d'un deuxième module EI, on peut gérer plusieurs applications. De plus, cela améliore la sécurité desdits modules, étant donné qu'un fraudeur aura plus de difficulté à, d'une part, découvrir une clef applicative parmi d'autres, et d'autre part, à savoir à qu'elle application elle est dédiée. Dans l'exemple précédent concernant le domaine de la fidélité, lors de

l'utilisation d'un deuxième module EI, celui-ci doit pouvoir fournir différentes prestations telles que la sécurisation des transactions de débit-crédit de points pour par exemple différents types de carburant. Il est ainsi important d'avoir différentes clefs applicatives TA dans ledit module EI pour gérer la sécurisation de ces différents types de transactions, ces derniers représentant différentes applications.

Aussi, dans une sixième étape, on envoie au deuxième module EI une information REF2 relative à une clef applicative TA, préalablement au déchiffrement dans ledit module EI de la clef applicative TA chiffrée, comme le montre la figure 4. L'information REF2 permet, soit de choisir la clef applicative TA qui va recevoir la valeur de la clef applicative provenant du premier module AS, soit d'indiquer un emplacement où sera chargée ladite clef TA provenant dudit premier module AS. Ainsi, on peut soit modifier une valeur d'une clef TA déjà existante dans ledit deuxième module EI, soit charger une nouvelle clef applicative TA dans le deuxième module EI pour une nouvelle application utilisateur.

Dans le cas où la clef applicative TA référencée par ladite information REF2 n'existe pas ou que ledit emplacement n'existe pas ou n'est pas fait pour accueillir une clef, le deuxième module EI rejette la clef reçue et indique qu'une erreur s'est produite. On notera que les informations REF1 et REF2 envoyées respectivement au premier et deuxième modules de sécurité peuvent être équivalentes.

Par la suite, lors d'une phase d'utilisation, une des clefs applicatives TA se trouvant dans le deuxième module EI pourra être utilisée par ledit module pour s'identifier vis-à-vis d'entités extérieures comme par exemple une carte utilisateur. Or ladite identification doit être unique. Par conséquent, ladite clef TA ne doit pas avoir de doublon. Aussi, lorsque l'on veut charger cette clef, on diversifie dans le premier module AS ladite clef applicative TA choisie, préalablement au

chiffrement de ladite clef. La diversification se fait en fonction d'une information propre à chaque deuxième module.

Enfin, dans une dernière étape, on enregistre dans le deuxième module EI, après le déchiffrement de la clef applicative TA chiffrée, ladite clef TA dans ledit module EI. L'enregistrement dans ledit deuxième module EI de la clef applicative TA se fait en fonction de l'information REF2 relative à une clef applicative TA. L'enregistrement se fait dans la mémoire M non volatile réinscriptible.

Le deuxième module EI peut maintenant être utilisé et être placé sur un site utilisateur distant tel qu'un terminal de stations service. On notera qu'aucune clef T1 d'exploitation n'a été transférée du premier module AS au deuxième module EI et n'a été enregistrée dans la mémoire M des modules de sécurité. Les opérations nécessaires à ces deux actions ne sont pas effectuées ce qui permet de gagner du temps lors de la phase de personnalisation. Ainsi, on ne mémorise pas une donnée secrète immédiatement utilisable par un algorithme ce qui empêche un fraudeur qui analyse ledit algorithme de découvrir ladite donnée. Ainsi, il est inutile pour le fraudeur d'espionner soit le réseau de communication soit les modules de sécurité afin de trouver la clef T1 d'exploitation utilisée.

Un autre avantage de l'objet de la présente invention se trouve dans le fait que l'information SN propre à chaque deuxième module EI de sécurité est unique. La clef T1 d'exploitation, qui est diversifiée c'est à dire calculée à partir de cette information, est par conséquent unique pour chaque module EI de sécurité. Par suite, la clef applicative TA chiffrée, qui est fonction de ladite clef T1 d'exploitation, n'est destinée qu'à un unique deuxième module EI destinataire ce qui renforce l'aspect sécuritaire de l'invention. Si un deuxième module EI n'a pas la même information SN que celle utilisée pour calculer la clef T1 d'exploitation dans le premier module AS et s'il reçoit ainsi une clef applicative TA qui

ne lui est pas destinée, il rejette ladite clef et indique qu'une erreur s'est produite.

D'autres aspects sécuritaires décrits ci-dessous sont couverts par l'objet de la présente invention.

L'objet de la présente invention prévoit une étape supplémentaire, montrée à la figure 4, selon laquelle on envoie au premier module AS un nombre aléatoire R issu du deuxième module EI, préalablement au chiffrement dans le premier module AS de la clef applicative TA. Les informations permettant, d'une part, de chiffrer la clef applicative TA dans le premier module AS, et, d'autre part, de déchiffrer dans le deuxième module EI la clef applicative TA chiffrée, comprennent le nombre aléatoire R issu du deuxième module EI. L'utilisation du nombre aléatoire R pour chiffrer et déchiffrer ladite clef applicative TA évite d'avoir une même valeur de chiffrement d'une clef applicative TA destinée à un deuxième module EI lorsque, par exemple, l'on charge plusieurs fois ladite clef dans ledit module. Ainsi, chaque chiffrement d'une clef applicative TA destinée à un deuxième module EI est unique. Ainsi, un fraudeur qui espionne le réseau de communication et récupère les données DONNEES lors du transfert n'obtient jamais une même valeur de chiffrement et ne peut par conséquent découvrir un secret relatif à la clef applicative TA transférée.

Cependant, lors dudit transfert, le fraudeur peut avoir effectué des opérations frauduleuses qui altèrent les données transférées. Aussi, on vérifie que les données DONNEES comprenant la clef applicative TA chiffrée sont intègres. A cette fin, comme le montre la figure 5, on calcule dans le premier module AS un certificat CAS sur lesdites données DONNEES, préalablement à l'envoi desdites données, ledit certificat étant envoyé par la suite au deuxième module EI et vérifié dans ledit deuxième module, préalablement au déchiffrement dans ledit deuxième module EI de la clef applicative TA chiffrée. Afin d'effectuer la

vérification, on calcule dans le deuxième module EI un certificat CEI en fonction des données reçues et on compare les deux certificats CAS et CEI. Si une fraude ou une erreur s'est produite lors dudit transfert, la vérification du certificat CAS est erronée, le déchiffrement de la clef applicative TA ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Ce système garantit ainsi une intégrité des données DONNEES lors de leur transfert depuis le premier module AS vers le deuxième module EI sur le réseau de communication et ce avant l'utilisation d'un deuxième module EI c'est à dire avant leur mise en circulation sur le terrain. De plus, dans le cas où la vérification serait fausse, cela évite de faire un déchiffrement inutile et par suite de perdre du temps inutilement.

De même qu'il faut garantir l'intégrité des données transférées, de même il faut garantir l'authenticité des données qui sont enregistrées dans le deuxième module EI. Ainsi, on vérifie que la clef applicative TA est authentique. A cet effet, comme le montre la figure 5, on calcule dans le premier module AS, préalablement au chiffrement de la clef applicative TA, une signature SAS de ladite clef TA, ladite signature étant envoyée par la suite au deuxième module EI et vérifiée dans ledit module. La vérification de la signature de ladite clef applicative TA se fait postérieurement au déchiffrement dans le deuxième module EI de ladite clef TA chiffrée et préalablement à l'enregistrement de ladite clef dans ledit module. Afin d'effectuer la vérification, on calcule dans le deuxième module EI une signature SEI avec la clef applicative TA déchiffrée dans ledit module EI et on compare les deux signatures SAS et SEI. Dans le cas où les deux signatures sont équivalentes, la clef applicative TA déchiffrée est authentique et est enregistrée. Dans le cas où la clef applicative TA n'est pas authentique, l'enregistrement de ladite clef ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Le système décrit ci-dessus permet ainsi de vérifier que

l'on récupère bien la clef applicative TA choisie dans le premier module AS et non une autre clef. On notera que lorsque ladite signature SAS existe, le certificat CAS est calculé également en fonction de ladite signature SAS. Ladite signature fait partie des données DONNEES envoyées lors de la troisième étape décrite précédemment.

L'envoi de données telles qu'un certificat ou une signature à un module de sécurité fait appel à des opérations dont le temps d'accomplissement s'ajoute à celui de la phase de personnalisation. Aussi, comme le montre la figure 6, afin de réduire le nombre d'accès aux différents modules et ainsi de réduire le temps de personnalisation, on envoie l'ensemble des données dont a besoin un module de sécurité en une seule fois au moyen d'une unique commande. Le nombre R aléatoire, le nombre REF1 relatif à une clef applicative TA et le nombre SN propre au deuxième module EI sont envoyés au premier module AS au moyen d'une unique première commande EXPORTKEY. De la même façon, la clef applicative TA chiffrée, le nombre REF2 relatif à une clef applicative TA, la signature SAS ainsi que le certificat CAS s'ils existent, sont envoyés au deuxième module EI au moyen d'une unique deuxième commande IMPORTKEY.

L'invention s'applique plus particulièrement dans le cas où le premier module AS de sécurité est une carte à puce. La carte à puce comprend un corps de carte plastique dans lequel est incorporé un module électronique comportant une puce à circuit intégré. Ladite puce comprend couramment deux mémoires M et une troisième mémoire volatile (RAM), la première mémoire M étant réinscriptible (EEPROM) et la deuxième non réinscriptible (ROM). La première mémoire M comprend l'ensemble des clefs applicatives TA et la clef de transport T. La troisième mémoire comprend la clef T1 d'exploitation. Celle-ci ne demeure dans ladite mémoire que le temps de chiffrement ou de déchiffrement de la clef applicative dans un module de sécurité. Les

algorithmes ALGO1 de diversification et ALGO2 de cryptage peuvent se trouver dans la première ou deuxième mémoire M. Cependant, on notera qu'il n'est pas obligatoire d'avoir lesdits algorithmes dans la carte à puce. Ils peuvent se trouver dans une entité extérieure à ladite carte à puce, par exemple dans une unité centrale d'un terminal avec lequel serait connectée ladite carte à puce.

La carte à puce permet d'assurer une meilleure protection des clefs applicatives TA. Dans une carte à puce, contrairement à un terminal d'un ordinateur par exemple, lesdites clefs sont inconnues de toute entité (d'un terminal, d'un administrateur de ladite carte, d'une autre carte à puce, ...) excepté de l'entité émettrice desdites clefs. De plus, une fraude est plus difficile à réaliser sur une carte à puce que sur une unité centrale d'un terminal par exemple. Pour les mêmes raisons, le deuxième module de sécurité est une carte à puce.

On notera qu'une clef applicative TA étant dans une mémoire M non volatile, elle peut être utilisée lors de plusieurs phases d'utilisation d'un deuxième module EI, car même lorsque ce dernier n'est plus alimenté, ladite clef n'est pas effacée.

REVENDICATIONS

1 - Procédé de personnalisation d'un ensemble (S) de plusieurs deuxièmes modules de sécurité (EI) comprenant un chargement sécurisé d'une clef applicative (TA) à partir d'un premier module (AS) de sécurité d'une unité centrale vers ledit ensemble de deuxièmes modules (EI) de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire (M), caractérisé en ce qu'il comporte les étapes selon lesquelles :

Pour chaque deuxième module (EI) dudit ensemble (S),

- lors de chaque chargement, on calcule dans le premier module (AS) une clef (T1) d'exploitation à partir d'une information propre au deuxième module (EI), d'une clef de transport (T) et d'un algorithme de diversification (ALGO1), ladite clef de transport (T) se trouvant dans la mémoire (M) du premier module de sécurité (AS), ladite mémoire (M) étant non volatile,
- on chiffre dans le premier module (AS) la clef (TA) applicative, à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme de cryptage (ALGO2), ladite clef (TA) applicative se trouvant dans ladite mémoire (M),
- on envoie au deuxième module (EI) des données (DONNEES) comprenant la clef (TA) applicative chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module (EI) la clef (T1) d'exploitation à partir de l'information propre au deuxième module (EI), de la clef de transport (T) et de l'algorithme de diversification (ALGO1), ladite même clef de transport (T) se trouvant dans la mémoire (M) non volatile de chaque deuxième module (EI) de sécurité dudit ensemble (S), ladite clef (T1) d'exploitation n'étant pas enregistrée dans la mémoire (M) dudit deuxième module,

- on déchiffre dans le deuxième module (EI) la clef applicative (TA) chiffrée, à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme de décryptage (ALGO2P) inverse de l'algorithme de cryptage (ALGO2).

2 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) l'information propre au deuxième module (EI), préalablement au calcul dans le premier module (AS) de la clef (T1) d'exploitation.

3 - Procédé selon les revendications 1 ou 2, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) un nombre aléatoire issu du deuxième module (EI), préalablement au chiffrement dans le premier module (AS) de la clef applicative (TA).

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) une information relative à une clef applicative (TA), préalablement au chiffrement dans ledit module (AS) de la clef applicative (TA).

5 - Procédé selon la revendication 4, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On choisit la clef applicative (TA) à chiffrer à partir de ladite information.

6 - Procédé selon l'une des revendications précédentes, caractérisé en ce que chaque chiffrement d'une clef applicative (TA) destinée à un deuxième module (EI) est unique.

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que les données (DONNEES) comprenant la clef applicative (TA) chiffrée sont intègres.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au deuxième module (EI) une information relative à une clef applicative (TA), préalablement au déchiffrement dans ledit module (EI) dudit ensemble (S) de la clef applicative (TA) chiffrée.

9 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On enregistre dans le deuxième module (EI), après le déchiffrement de la clef applicative (TA) chiffrée, ladite clef (TA) dans ledit module (EI).

10 - Procédé selon la revendication 9, caractérisé en ce que l'enregistrement dans ledit deuxième module (EI) de la clef applicative (TA) se fait en fonction de l'information relative à une clef applicative (TA).

11 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que la clef applicative (TA) est authentique.

12 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le premier module de sécurité (AS) est une carte à puce.

13 - Procédé selon l'une des revendications précédentes, caractérisé en ce que la mémoire (M) est une mémoire réinscriptible.

14 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'un deuxième module (EI) comprend plusieurs clefs applicatives (TA).

15 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le premier module (AS) comporte plusieurs clefs applicatives (TA).

16 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- Postérieurement au chiffrement de la clef applicative (TA), on efface la clef (T1) d'exploitation sauvegardée temporairement dans une deuxième mémoire volatile du premier module (AS).

17 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- Postérieurement au déchiffrement de la clef applicative (TA), on efface la clef (T1) d'exploitation sauvegardée temporairement dans une deuxième mémoire (M2) volatile du deuxième module (EI).

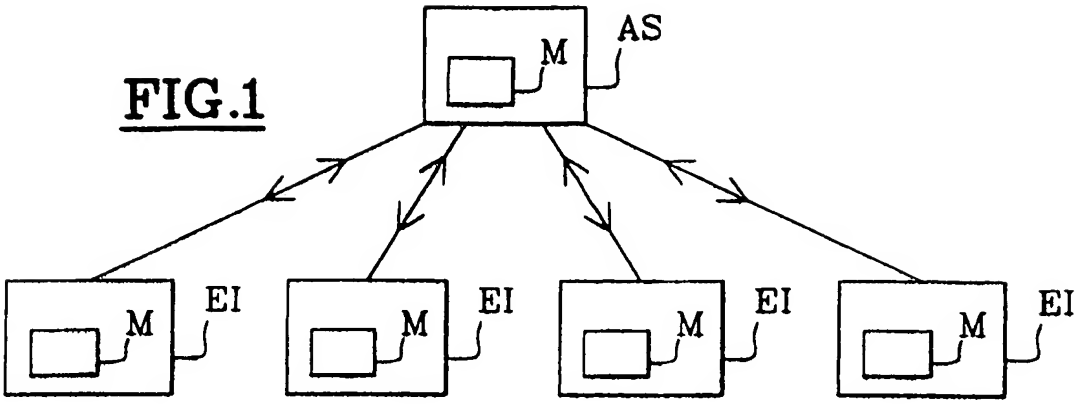
18 - Procédé selon les revendications 2 à 4 précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- L'information aléatoire, l'information relative (REF1) à une clef applicative (TA) et l'information (SN) propre au deuxième module (EI) sont envoyées au premier module (AS) au moyen d'une unique première commande (EXPORTKEY).

19 - Procédé selon les revendications 1 et 2 précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- La clef applicative (TA) chiffrée et l'information (REF2) relative à une clef applicative (TA), sont envoyées au deuxième module (EI) au moyen d'une unique deuxième commande (IMPORTKEY).

FIG.1



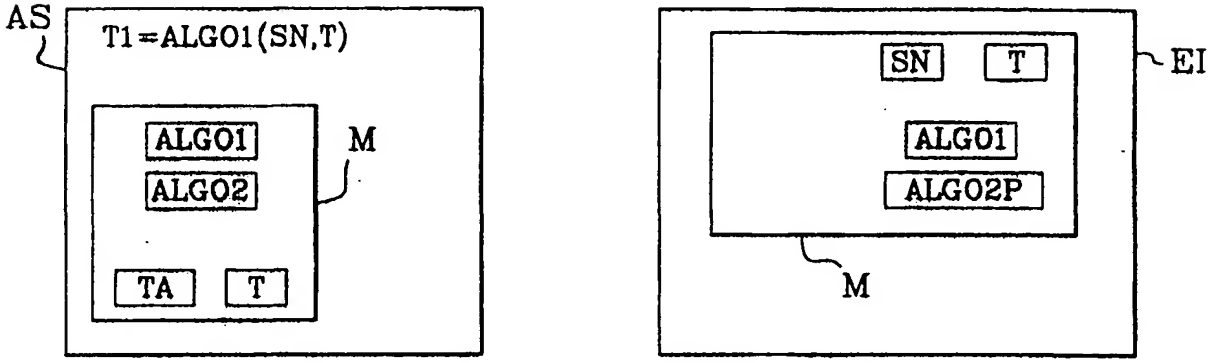


FIG.2

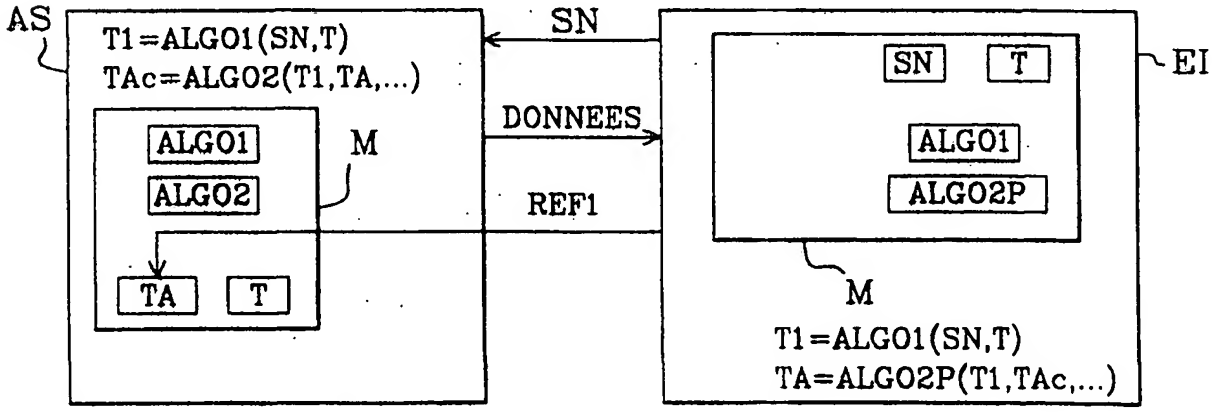


FIG.3

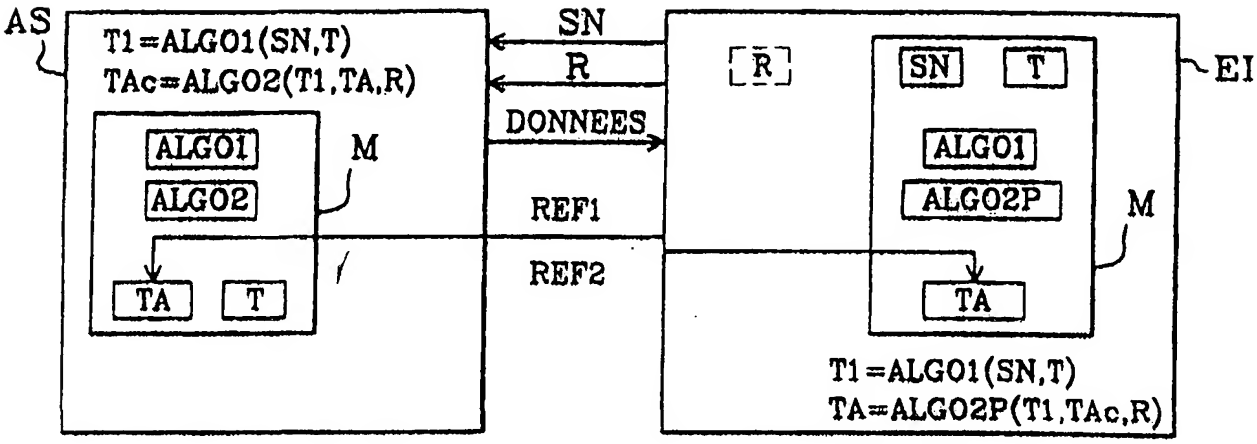

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
M
TA
T
SN
R
DONNEES
REF1
REF2
R
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.4

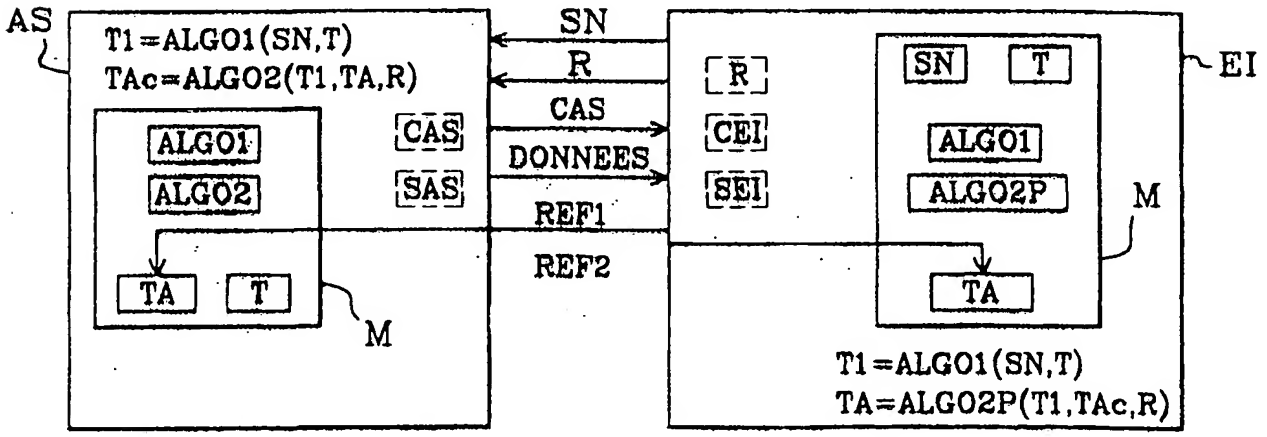

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
SN
R
CAS
DONNEES
REF1
REF2
R
CEI
SEI
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.5

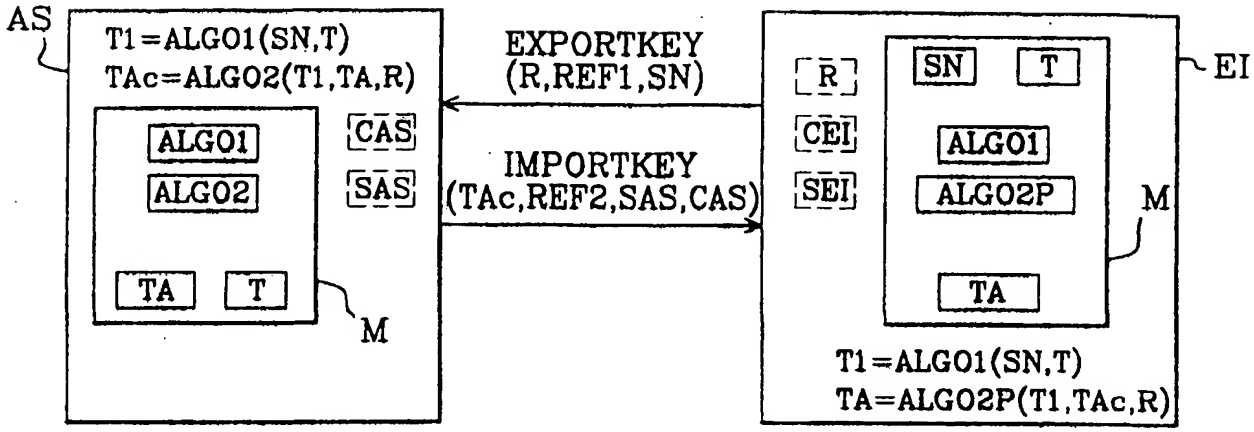

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
EXPORTKEY
(R,REF1,SN)
IMPORTKEY
(TAc,REF2,SAS,CAS)
R
CEI
SEI
SN
T
ALGO1
ALGO2P
TA
M
EI
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.6

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 517 567 A (EPSTEIN PHILIP) 14 May 1996 (1996-05-14) cited in the application column 5, line 55 -column 7, line 40 column 8, line 5 - line 10 ---	1,3,6,9
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract page 5, line 17 - line 30 page 6, line 27 -page 7, line 12 page 7, line 20 -page 10, line 18 ---	1,3,6,9 12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 July 1997 (1997-07-10) abstract page 9, line 13 - line 23 --- -/--	1,4,5

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 April 2000	11/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

3

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 December 1997 (1997-12-11) page 6, line 17 - line 22 page 12, line 29 -page 14, line 2 ---	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 December 1995 (1995-12-27) abstract figure 1 ---	1,7
A	EP 0 725 512 A (IBM) 7 August 1996 (1996-08-07) column 10, last paragraph -column 11, line 10; claim 1 -----	16,17

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5517567 A	14-05-1996	NONE	
FR 2681165 A	12-03-1993	NONE	
WO 9724831 A	10-07-1997	AU 1425197 A	28-07-1997
WO 9747109 A	11-12-1997	CN 1227686 A	01-09-1999
		EP 0903026 A	24-03-1999
EP 0688929 A	27-12-1995	US 5686904 A	11-11-1997
		ZA 9505429 A	13-02-1996
EP 0725512 A	07-08-1996	US 5604801 A	18-02-1997
		JP 8340330 A	24-12-1996

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) cité dans la demande colonne 5, ligne 55 -colonne 7, ligne 40 colonne 8, ligne 5 - ligne 10 ---	1,3,6,9
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) abrégé	1,3,6,9
A	page 5, ligne 17 - ligne 30 page 6, ligne 27 -page 7, ligne 12 page 7, ligne 20 -page 10, ligne 18 ---	12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 juillet 1997 (1997-07-10) abrégé page 9, ligne 13 - ligne 23 --- -/--	1,4,5

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
5 avril 2000	11/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

3

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 décembre 1997 (1997-12-11) page 6, ligne 17 - ligne 22 page 12, ligne 29 -page 14, ligne 2 ---	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 décembre 1995 (1995-12-27) abrégé figure 1 ---	1,7
A	EP 0 725 512 A (IBM) 7 août 1996 (1996-08-07) colonne 10, dernier alinéa -colonne 11, ligne 10; revendication 1 -----	16,17

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5517567 A	14-05-1996	AUCUN	
FR 2681165 A	12-03-1993	AUCUN	
WO 9724831 A	10-07-1997	AU 1425197 A	28-07-1997
WO 9747109 A	11-12-1997	CN 1227686 A	01-09-1999
		EP 0903026 A	24-03-1999
EP 0688929 A	27-12-1995	US 5686904 A	11-11-1997
		ZA 9505429 A	13-02-1996
EP 0725512 A	07-08-1996	US 5604801 A	18-02-1997
		JP 8340330 A	24-12-1996

)